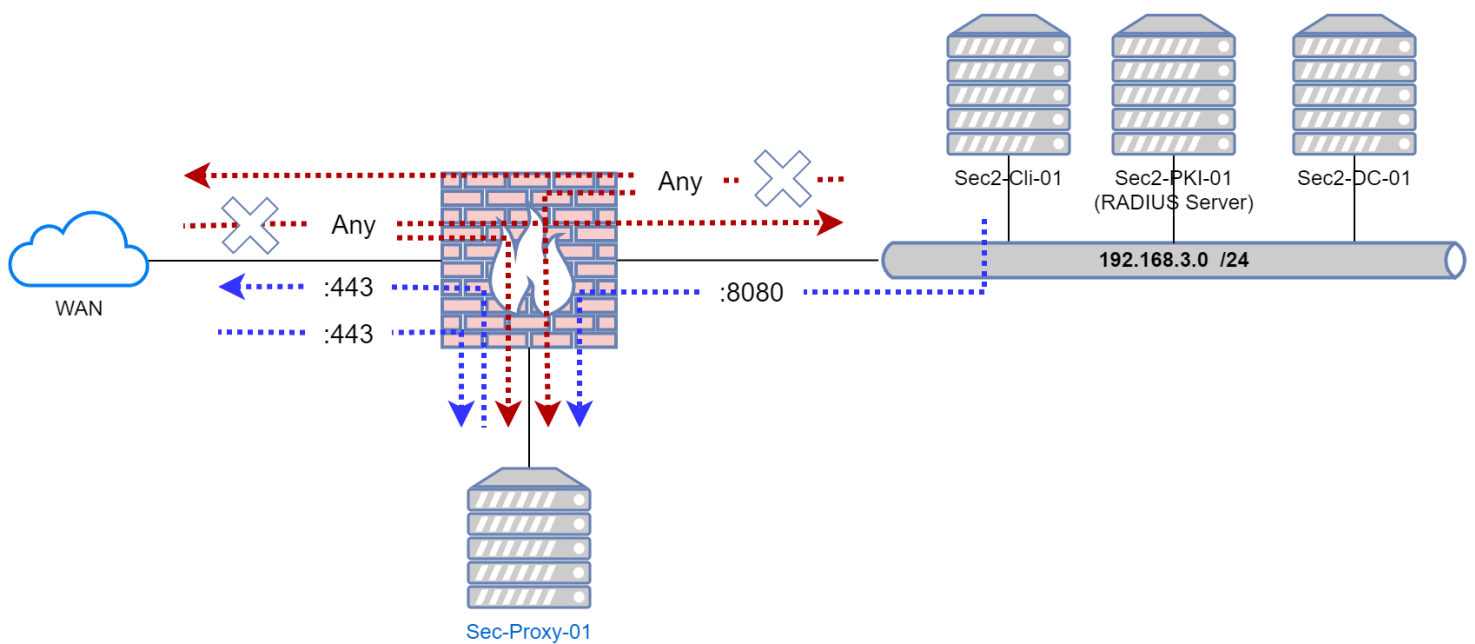


POC DMZ, rapport mise en service

Table des matières

POC DMZ, rapport mise en service	1
Schéma de l'infra :	1
User Story 1	2
User Story 2	2
User Story 3	2
User Story 4	3
User Story 5	4
User Story 6	4

Schéma de l'infra :



User Story 1

En tant qu'utilisateur du LAN j'aimerais accéder à Internet de manière sécurisée dans le but de ne pas compromettre la sécurité de mon entreprise.

Copie d'écran de la config du proxy dans le navigateur

```
auth_param basic program /usr/lib/squid/basic_radius_auth -f /etc/radius_config
auth_param basic children 5
auth_param basic realm Web-Proxy
auth_param basic credentialsttl 5 minute
auth_param basic casesensitive off

acl radius-auth proxy_auth REQUIRED

acl whitelist dstdomain "/etc/squid/sites.whitelist.txt"

acl lannet src 192.168.3.0/24

http_access allow lannet radius-auth whitelist
http_access deny all

http_port 8080
```

User Story 2

En tant qu'utilisateur du LAN j'aimerais que mon navigateur soit configuré de manière automatique au niveau du proxy à utiliser, dans le but de se simplifier la vie.

Copie d'écran de la GPO

Section GPO en fin de rapport

Copie d'écran du contenu du proxy.pac

User Story 3

En tant que responsable de la sécurité, j'aimerais que les machines de mon infrastructure puissent communiquer en respectant les principes d'une DMZ, dans le but de sécuriser mon infrastructure contre la compromission d'une ou plusieurs machines.

Tableau des règles du firewall :

Source	Destination	Protocol	Action

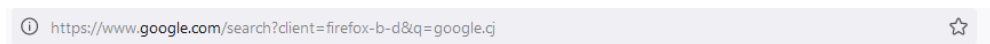
Section Regles en fin de rapport

Image avec les règles du firewall, (onglet Filter Rules de IP Firewall sur Winbox), mettez des commentaires dans les règles afin d'éclaircir la lecture

Section Regles en fin de rapport

User Story 4

En tant que CTO, j'aimerais que les utilisateurs du LAN puissent surfer sur un nombre restreint de sites (www.cpnv.ch, www.vd.ch), pour améliorer leur productivité.

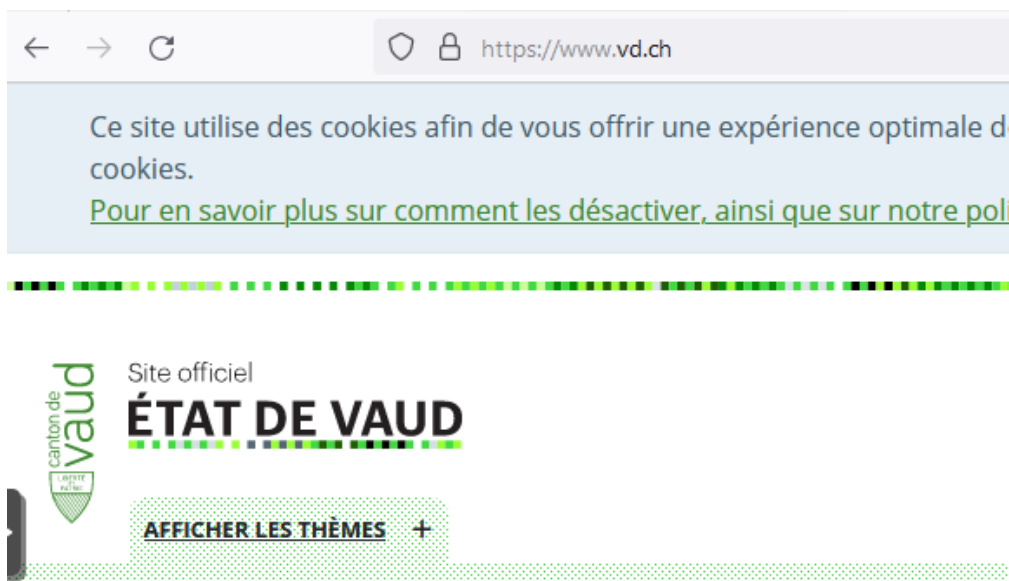


La connexion a été refusée par le serveur proxy

Une erreur est survenue pendant une connexion à www.google.com.

- Vérifiez que les paramètres du proxy sont corrects ;
- Contactez votre administrateur réseau pour vous assurer que le serveur proxy fonctionne.

Réessayer



```

1701370946.057 106348 192.168.3.50 TCP_TUNNEL/200 4872 CONNECT incoming.telemetry.mozilla.org:443 user1 HIER_DIRECT/34.120.208.123 -
1701370946.107 0 192.168.3.50 TCP_DENIED/403 4460 POST http://ocsp.swisssign.net/DA34048E1023F46A2D6CB41FF32811DE5E01C4DE user1 HIER_NONE/- text/html
1701370946.371 0 192.168.3.50 TCP_DENIED/403 4460 POST http://ocsp.swisssign.net/DA34048E1023F46A2D6CB41FF32811DE5E01C4DE user1 HIER_NONE/- text/html
1701370946.372 0 192.168.3.50 TCP_DENIED/403 4110 CONNECT www.googletagmanager.com:443 user1 HIER_NONE/- text/html
1701370946.374 0 192.168.3.50 TCP_DENIED/403 4460 POST http://ocsp.swisssign.net/DA34048E1023F46A2D6CB41FF32811DE5E01C4DE user1 HIER_NONE/- text/html
1701370946.381 0 192.168.3.50 TCP_DENIED/403 4460 POST http://ocsp.swisssign.net/DA34048E1023F46A2D6CB41FF32811DE5E01C4DE user1 HIER_NONE/- text/html
1701370946.394 0 192.168.3.50 TCP_DENIED/403 4460 POST http://ocsp.swisssign.net/DA34048E1023F46A2D6CB41FF32811DE5E01C4DE user1 HIER_NONE/- text/html
1701370946.419 0 192.168.3.50 TCP_DENIED/403 4460 POST http://ocsp.swisssign.net/DA34048E1023F46A2D6CB41FF32811DE5E01C4DE user1 HIER_NONE/- text/html
1701370946.458 0 192.168.3.50 TCP_DENIED/403 4460 POST http://ocsp.swisssign.net/ACD03AC2C25755916911CC706A59388A8CAC9C3D user1 HIER_NONE/- text/html
1701370946.655 0 192.168.3.50 TCP_DENIED/403 4460 POST http://ocsp.swisssign.net/DA34048E1023F46A2D6CB41FF32811DE5E01C4DE user1 HIER_NONE/- text/html
1701370946.665 58 192.168.3.50 TCP_TUNNEL/200 8981 CONNECT prestations.vd.ch:443 user1 HIER_DIRECT/145.232.192.146 -
1701370946.676 0 192.168.3.50 TCP_DENIED/403 4110 CONNECT www.google-analytics.com:443 user1 HIER_NONE/- text/html
1701370949.858 3486 192.168.3.50 TCP_TUNNEL/200 74533 CONNECT statsweb.vd.ch:443 user1 HIER_DIRECT/145.232.192.131 -
1701370949.858 3537 192.168.3.50 TCP_TUNNEL/200 260010 CONNECT www.vd.ch:443 user1 HIER_DIRECT/145.232.192.197 -
1701370949.858 3538 192.168.3.50 TCP_TUNNEL/200 550765 CONNECT www.vd.ch:443 user1 HIER_DIRECT/145.232.192.197 -
1701370949.859 3544 192.168.3.50 TCP_TUNNEL/200 27576 CONNECT www.vd.ch:443 user1 HIER_DIRECT/145.232.192.197 -
1701370949.859 3546 192.168.3.50 TCP_TUNNEL/200 215750 CONNECT www.vd.ch:443 user1 HIER_DIRECT/145.232.192.197 -
1701370949.859 3547 192.168.3.50 TCP_TUNNEL/200 1117901 CONNECT www.vd.ch:443 user1 HIER_DIRECT/145.232.192.197 -
1701370949.859 3799 192.168.3.50 TCP_TUNNEL/200 290442 CONNECT www.vd.ch:443 user1 HIER_DIRECT/145.232.192.197 -
1701370949.862 0 192.168.3.50 TCP_DENIED/403 4080 CONNECT www.google.com:443 user1 HIER_NONE/- text/html

```

User Story 5

En tant que responsable de la sécurité, j'aimerais que le LAN puisse accéder au WAN uniquement à l'aide de ping et protocoles web (https, http), dans le but de protéger l'infrastructure

```

C:\Users\user1>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=54
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=54

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 7ms, Maximum = 7ms, Moyenne = 7ms
    ...

```

User Story 6

En tant que responsable informatique, je veux que les internautes puissent avoir accès à un site web dans le DMZ qui réponde à http://iam.secuxx.internal, dans le but de par la suite mettre en place un service d'authentification.

Image avec les règles du firewall, (onglet Nat Rules de IP Firewall sur Winbox), mettez des commentaires dans les règles afin d'éclaircir la lecture

Firewall: NAT: Port Forward										Select category
	Interface	Proto	Source Address	Source Ports	Destination Address	Destination Ports	NAT IP	Ports	Description	
<input type="checkbox"/>	LAN	TCP	*	*	LAN address	80, 5000	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	WAN	TCP	*	*	WAN net	2222	192.168.42.10	22 (SSH)	Port Forward SSH for Proxy Management	
<input type="checkbox"/>	WAN	TCP	*	*	WAN net	443 (HTTPS)	192.168.42.10	443 (HTTPS)	Port Forward HTTPS for WebSite Access	
<input checked="" type="checkbox"/>	Enabled rule				<input checked="" type="checkbox"/> No redirect				<input checked="" type="checkbox"/> Linked rule	
<input type="checkbox"/>	Disabled rule				<input type="checkbox"/> Disabled no redirect				<input type="checkbox"/> Disabled linked rule	

Section GPO

Nom	Ordre	Action	Ruche	Clé	Nom de valeur	Type	Données de valeur
ProxyEnable	1	Mettre ...	HKEY_CURRENT_USER	Software\Microsoft\...	ProxyEnable	REG_DWORD	00000001
ProxyOverride	3	Mettre ...	HKEY_CURRENT_USER	Software\Microsoft\...	ProxyOverride	REG_SZ	192.168.3.*
ProxyServer	2	Mettre ...	HKEY_CURRENT_USER	Software\Microsoft\...	ProxyServer	REG_SZ	192.168.42.10:8080

Propriétés de : ProxyEnable

Général

Commun

Action :

Mettre à jour

Ruche :

HKEY_CURRENT_USER

Chemin d'accès de la clé :

Software\Microsoft\Windows\CurrentV

...

Nom de valeur

☐ Par défaut

ProxyEnable

Type de valeur :

REG_DWORD

Données de valeur :

1

Base

☐ Hexadécimal

☒ Décimal

OK

Annuler

Appliquer

Aide

Propriétés de : ProxyOverride

Général

Commun

Action :

Mettre à jour

Ruche :

HKEY_CURRENT_USER

Chemin d'accès de la clé :

Software\Microsoft\Windows\CurrentV

...

Nom de valeur

☐ Par défaut

ProxyOverride

Type de valeur :

REG_SZ

Données de valeur :

192.168.3.*

OK

Annuler

Appliquer

Aide

Propriétés de : ProxyServer

Général

Commun

Action :

Mettre à jour

Ruche :

HKEY_CURRENT_USER

Chemin d'accès de la clé :

Software\Microsoft\Windows\CurrentV

...

Nom de valeur

☐ Par défaut

ProxyServer

Type de valeur :

REG_SZ

Données de valeur :

192.168.42.10:8080

OK

Annuler

Appliquer

Aide

PARAMÈTRES UTILISATEURS

CN=user1,CN=Users,DC=secu03,DC=local
Heure de la dernière application de la stratégie de groupe : 30.11.2023 à 19:22:48
Stratégie de groupe appliquée depuis : sec2-dc-01.secu03.local
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : SECU03
Type de domaine : Windows 2008 ou supérieur

Objets Stratégie de groupe appliqués

proxy_settings

Proxy

Enregistrer

Configuration manuelle du proxy

Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.

Utiliser un serveur proxy



Activé

Adresse

192.168.42.10

Port

8080

Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.

192.168.3.*



Ne pas utiliser le serveur proxy pour les adresses (intranet) locales















Enregistrer

Regles

Source	Destination	Protocol	Action
WAN	DMZ	HTTPS	Pass
WAN	LAN	ICMP (ping reply)	Pass
WAN	any	any	Block
DMZ	DMZ (Interface address)	DNS	Pass
DMZ	! LAN (All)	any	Pass
DMZ	LAN (Radius Server Address)	RADIUS 1812	Pass
DMZ	LAN (Radius Server Address)	RADIUS 1813	Pass
DMZ	any	any	Block
LAN	DMZ Network	Custom (8080)	Pass
LAN	any	ICMP (ping request)	Pass
LAN	any	any	Block


















Firewall: Rules: WAN

Select category

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description 
<input type="checkbox"/>	Automatically generated rules								
<input type="checkbox"/>	   IPv4 TCP	*	*	192.168.42.10	443 (HTTPS)	*	*		Port Forward HTTPS for WebSite Access
<input type="checkbox"/>	   IPv4 TCP	*	*	192.168.42.10	22 (SSH)	*	*		Port Forward SSH for Proxy Management
<input type="checkbox"/>	   IPv4 TCP/UDP	*	*	WAN address	5000	*	*		Allow requests on port 5000 to WAN address
<input type="checkbox"/>	   IPv4 ICMP	WAN net	*	LAN net	*	*	*		Allow ICMP ping reply to LAN Net















Firewall: Rules: DMZ

Select category

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description 
<input type="checkbox"/>	Automatically generated rules								
<input type="checkbox"/>	   IPv4 TCP/UDP	DMZ net	*	DMZ address	53 (DNS)	*	*		Allow access to DNS server
<input type="checkbox"/>	   IPv4 TCP/UDP	DMZ net	*	*	53 (DNS)	*	*		Block access to all other DNS servers
<input type="checkbox"/>	   IPv4 TCP/UDP	DMZ net	*	192.168.3.11	1812 (RADIUS)	*	*		Allow access to RADIUS server Authentication
<input type="checkbox"/>	   IPv4 TCP/UDP	DMZ net	*	192.168.3.11	1813 (RADIUS accounting)	*	*		Allow access to RADIUS server Accounting
<input type="checkbox"/>	   IPv4 TCP/UDP	DMZ net	*	! LAN net	443 (HTTPS)	*	*		Allow access to Internet and block access to all local networks

Firewall: Rules: LAN

Select category

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description 
<input type="checkbox"/>	Automatically generated rules								
<input type="checkbox"/>	   IPv4 TCP/UDP	LAN net	*	DMZ net	8080	*	*		Allow 8080 request to DMZ
<input type="checkbox"/>	   IPv4 TCP/UDP	LAN net	*	LAN address	5000	*	*		Allow Opnsense managment from Lan
<input type="checkbox"/>	   IPv4 ICMP	LAN net	*	*	*	*	*		Allow ICMP ping request to any
<input type="checkbox"/>	   IPv4 *	*	*	*	*	*	*		Allow all request to any

